

# XML

## DEFENSICS for XML

During the past years, XML adoption has spread rapidly reaching almost every area of business and society. XML is not a protocol in itself, but a versatile method for describing structures. It can be used for almost any purpose, hence its popularity in modern protocols, file formats and applications; there is hardly an industry where XML is not used. Here also lie the biggest security risks: versatile technologies tend to create complexity, which is a breeding ground for security vulnerabilities, in addition, the fast adoption and the diversity of use cases have overwhelmed traditional security testing and few or no security testing solutions for XML have been available to customers, until now.

### Codonomicon Introduces XML Fuzzing

Early 2009 Codonomicon took the first steps in intelligent XML fuzz testing by introducing tests for the CWMP (TR-69) protocol. The product selection quickly expanded to include a general purpose XML security testing solution, which spans both standard and custom XML based protocols. The extent and magnitude of the vulnerabilities we discovered during the development of XML fuzzing reminded us of our earlier experience with ASN.1 vulnerabilities (2001-2002 PROTOS SNMP). Testing a multi-purpose technology like XML for security is challenging, but at Codonomicon we have a long background in fuzz testing.



*Codonomicon has found a critical focus area which expands beyond web testing, where the XML industry has an opportunity to proactively assess the security holes contained in everyday services used by the general public. I would hope the industry warmly welcomes both the research results and an innovative testing solution to help diagnose the problems.*

- Prof. Howard A. Schmidt, former White House Cyber Security advisor & Codonomicon board member

### DEFENSICS Test Solution

The Codonomicon DEFENSICS test platform provides **solutions for preemptive security and robustness testing** for a wide variety of systems and services ranging from consumer electronics to high end network devices and operator environments. In robustness testing, or fuzzing, large amounts of intentionally malformed test vectors are sent to the system under test, while the behavior of the system is monitored under the unexpected inputs. By simulating attack scenarios and malfunction conditions, systems can be hardened before their commercial deployment.

DEFENSICS is the most effective **automated negative black-box testing solution** in the market for developers, service providers and enterprises seeking to mitigate security exposure and system failure risks in their applications, devices and services. Model-based fully stateful fuzzing guarantees thorough input space coverage and also addresses problematic corner cases. DEFENSICS supports over 150 different protocols and media formats, an unparalleled achievement in the security testing market. With the introduction of XML support, DEFENSICS became the only solution covering the whole application stack from Layer 2 to the Application layer, even including often vulnerable Digital Media processing and Wireless interfaces.

According to independent studies, the Codonomicon DEFENSICS security and robustness test platform remains unmatched in its ability to find quality, resiliency and security exposures quickly within a broad array of applications. Codonomicon is recognized in the industry for its innovations in negative black-box testing. These capabilities are demonstrated by our unique test methodology, which is not only rigorous and systematic, but also enables repeatable tests.

